TOSTRUD LAW GROUP, P.C.
JON A. TOSTRUD
jtostrud@tostrudlaw.com
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600

KOHN, SWIFT & GRAF, P.C.
DENIS F. SHEILS (pro hac vice)
dsheils@kohnswift.com
BARBARA L. GIBSON (pro hac vice)
bgibson@kohnswift.com
1600 Market Street, Suite 2500
Philadelphia, PA 19103
Telephone: (215) 238-1700

Attorneys for Plaintiff Teresa J. McGarry and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

TERESA J. MCGARRY, on behalf of herself and all others similarly situated, Plaintiff, v. DELTA AIR LINES, INC., and [24]7.AI, INC., Defendants.	CASE NO. 2:18-cv-09827-MWF-E **CLASS ACTION** AMENDED CLASS ACTION COMPLAINT **DEMAND FOR JURY TRIAL**

Plaintiff Teresa J. McGarry, on behalf of herself and all others similarly situated, brings this Amended Class Action Complaint against Defendants, Delta Air Lines, Inc. ("Delta") and [24]7.AI, Inc. ("[24]7.ai") (collectively, "Defendants"). Plaintiff alleges the following on information and belief, except allegations as to her own actions are based on personal knowledge.

I. SUMMARY OF THE CASE

1. Plaintiff brings this action against Defendants Delta and [24]7.ai, a chat service that Delta retained to interact with customers through its website, for their failure to protect the highly confidential information of their customers, including Plaintiff. Due to a malware attack against [24]7.ai, hundreds of thousands of Delta customers (as well as additional customers of other, non-airline, [24]7.ai clients) had their credit and debit card account numbers, card verification codes, and expiration dates (collectively "Payment Card Data" or "PCD"), as well as their full names, mailing addresses, and potentially other information ("personally identifiable information" or "PII," collectively with PCD, "Customer Data"), exposed to malicious agents. Delta and [24]7.ai both failed to take appropriate precautions against the foreseeable eventuality of a malware attack and, after the attack occurred, failed to provide accurate and timely notification of the breach to Plaintiff and the Class. Indeed, Plaintiff and the Class members were not informed of the breach until nearly six months after the malware attack, during which period they did not know their Customer Data had been exposed and continued to be at risk. As a result, Defendants needlessly exposed Plaintiff and Class members to significant harm in the form of identity theft, potential false charges, and cost of measures to address this exposure of personal information, in violation of their contractual, statutory and common law obligations.

2. Delta, a major airline, interacts with customers extensively through its website. It obtains highly sensitive Customer Data that is of great value to hackers, identity thieves, and other criminal elements. Customer Data is personal property

belonging to the customer and Delta is obligated to take appropriate measures to safeguard this information. Instead, Delta improperly passed such information, including credit and debit account numbers and security codes, along to an undisclosed third party, [24]7.ai, without its customers' knowledge or informed consent. Moreover, Delta did not ensure that [24]7.ai was itself taking appropriate measures to protect Delta's customers' Customer Data; and, it failed to properly monitor [24]7.ai such that it failed to catch the Data Breach prior to the date [24]7.ai eventually notified Delta, which, according to Delta, itself was six months after the malware attack. The protection of customers' internet privacy is an obligation of every company that conducts business online. Protecting Customer Data has no demonstrable impact on or relationship to an air carrier's prices, schedules, or routes, and is as significant an obligation for Delta as for any other company whatever the industry.

3. [24]7.ai is a customer experience software and services company that specializes in providing chat agent, voice and artificial intelligence services. It handles more than 200 million virtual agent inquiries per year and more than 40 million agent chats per year for its clients. Aside from Delta, [24]7.ai also provides services to businesses in fields ranging from e-retail (including Best Buy, Sears, and others) to education to healthcare. As a technology company that describes itself as "[u]sing intent-driven engagement and deep chat analytics to understand what your customers want to do,"[1] which thus necessarily gathers, stores, and analyzes Customer Data as a core component of its business, [24]7.ai should be held to the highest standard of data security requirements.

4. On April 5, 2018, Delta disclosed that a malware attack had occurred at [24]7.ai approximately six months earlier -- between September 26 and October 12, 2017 (the "Data Breach"). It revealed that during that period, Customer Data

[1] https://www.247.ai/customer-engagement/247-chat

of the end users of certain of [24]7.ai clients' websites, including Delta's website, may have been accessed.

5. Delta also stated that a customer need not have even used the chat service on its website for his or her information to have been compromised.[2] Delta had no legitimate reason, much less a reason that impacts its prices, schedules or routes, to provide Customer Data to a third party chat service for customers that did not use that service, and its doing so needlessly exposed Plaintiff and hundreds of thousands of other Class members to harm. Moreover, the fact that consumers *could* complete their transactions without use of the chat service shows that [24]7.ai was not essential to *any* ticket sale transaction.

6. Delta has also stated that [24]7.ai discovered the breach in October 2017, but did not disclose it to Delta until late March 2018. This means that, at a minimum, one of Defendants ([24]7.ai) knew of the data breach for nearly six months before it disclosed that it happened, needlessly exposing customers to the undisclosed risk that that their Customer Data was or could be stolen and used. If true, this also indicates that Delta failed to properly monitor [24]7.ai with respect to security measures in not discovering the breach for such an extended period.

7. Plaintiff and hundreds of thousands of other customers who used the Delta website now face extensive risks and damages relating to identity theft due to each Defendant's failure to properly safeguard their confidential Customer Data.

II. PARTIES

8. Plaintiff Teresa J. McGarry ("Plaintiff") is a resident of Florida and booked airline tickets on the Delta website during the time of the breach. Plaintiff would not have purchased the tickets through the website if she had known that Delta had not taken adequate precautions to protect her confidential information or

[2] https://www.delta.com/content/www/en_US/response.html (last visited Jan. 21, 2019.)

if she had known that [24]7.ai would receive her data and that it had not taken adequate actions to protect it. Plaintiff received a letter from Delta notifying her of the Data Breach.

9. Defendant Delta is a major American airline. Delta is a Delaware limited liability company with a principal place of business at 1030 Delta Boulevard, Atlanta, Georgia 30320. Delta maintains and operates a website where customers can book tickets for airline travel online. Delta provides air transportation for passengers in the United States and abroad. Delta offers its services through a system of hubs from Atlanta, Boston, Detroit, Los Angeles, Minneapolis-St. Paul, New York, Salt Lake City, Seattle, and a number of international gateways, with its largest hub in Atlanta, Georgia.

10. Defendant [24]7.ai is a California corporation with its headquarters at 2001 Logic Drive, San Jose, CA 95124. [24]7.ai is a customer experience software and services company with approximately 12,000 employees. [24]7.ai *inter alia* provides online chat services for numerous major companies in various industries, including Delta, and collects end user data. 24/7 Customer Philippines is a division, service center, and/or other business component controlled by Defendant [24]7.ai, through which Defendant [24]7.ai provides services, including to Delta.

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over the claims asserted here pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a state different from any Defendant and, upon the original filing of this complaint, members of the putative Plaintiff class resided in states around the country; there are more than 100 putative class members; and the amount in controversy exceeds $5 million.

12. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because this is a civil action arising under the laws of the United States and pursuant to principles of supplemental jurisdiction in

accordance with 28 U.S.C. § 1367.

13. The Court also has personal jurisdiction over the Parties because Defendant Delta maintains a hub at Los Angeles International Airport and conducts a major part of its national operations with regular and continuous business activity in this district.

14. The Court has personal jurisdiction over [24]7.ai because its headquarters are in California and it conducts substantial business in and directed from the state.

15. In addition, Defendants' actions resulted in this litigation being moved to this Court from the Northern District of Georgia. Defendants therefore consented to this Court's jurisdiction.

16. Venue is based on the November 20, 2018 order of the Hon. Thomas W. Thrash, Jr. of the United States District Court for the Northern District of Georgia (where Plaintiff originally filed her action) which transferred this action to the Central District of California. D.E. No. 35. However, Judge Thrash, at page 13 of his ruling, noted that it is for this Court to determine whether this case should have been transferred to this Court.

IV. ALLEGATIONS

A. Data Privacy

17. Today, rapidly evolving Internet and other electronic technologies have created sophisticated opportunities for companies to gather, use and retain customer information.[3] Companies gather not only PII but also information about a person's habits such as their location, time of purchase and what webpages they visited on the website at the time of purchase.[4] This information is stored long

[3] *Proskauer on Privacy*, Remarks by FTC Comm. Julie Brill, Oct. 10, 2010 at 2.
[4] J. Valentino-Devries, N. Singer, M. H. Keller And A. Krolik, *Your Apps Know Where You Were Last Night, And They're Not Keeping It Secret*, N.Y. Times; Dec.

after the customer and company have completed the transaction and it is retained by the company for use in the future.

18. Sometimes this data is also monetized and sold while the customer is unaware. "[C]ompanies sell, use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior. It's a hot market, with sales of location-targeted advertising reaching an $21 billion this year." [5] "Every online purchase and credit card transaction, social media post, shared selfie and location ping from a smartphone is likely being used to help a company make money."[6] "There's tremendous economic value that's collectively created … All the data we generate every time we interact on any kind of digital platform is monetized."[7]

19. Companies also benefit from Customer Data they gather by using the data to train artificial intelligence systems, in targeted marketing, and to create data sets that they can analyze.[8] "All this is so new that ordinary people haven't figured out how manipulated they are by these companies."[9]

20. However, Customer Data is personal property belonging to the

---

10, 2018, available at: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (last visited Feb. 20, 2019).

[5] *Id.*

[6] Heather Kelly, *Companies Use Your Data To Make Money. California Thinks You Should Get Paid,* CNN Business, Feb. 13, 2019 available at: https://www.cnn.com/2019/02/13/tech/digital-dividend-california/index.html (last visited Feb. 21, 2019).

[7] *Id.*

[8] *Id.*

[9] Eduardo Porter, *Your Data is Crucial to a Robotic Age. Shouldn't You be Paid for It?*, N.Y. Times, March 6, 2018, available at: https://www.nytimes.com/2018/03/06/business/economy/user-data-pay.html (last visited Feb. 20, 2019).

customer. It is not a free byproduct of an Internet transaction that a company may use indefinitely however it chooses.

21. Or, put another way, just because a consumer provides personal information to a business for a limited purpose, it does not mean the business owns the information outright.

22. Customers are put at risk of identity theft and fraud for as long as the data is stored.

23. Hackers are aware of the vast amount of sensitive personal data stored on the Internet. Personal information is easily used to create fake accounts and take out fake loans, receive tax returns, and make fraudulent purchases.

24. Transmitting this information to third parties such as [24]7.ai creates a data risk and indefinite storage on a server creates a data risk. All of this additional data collection is largely unbeknownst to the consumers as end users of companies' websites.

25. On top of this already uneven playing field, companies like Delta attempt to invoke additional protections such as the Airline Deregulation Act ("ADA"), 49 U.S.C. § 1301 *et seq.*, to further protect their data collection practices from scrutiny. Chat services, such as that provided by [24]7.ai, were not even in existence at the time the ADA was enacted in 1978. Invoking the ADA in instances such as this will only embolden Delta, [24]7.ai and many other companies to continue to grab data for their own benefit while putting Customer Data at risk. Protecting airlines and third party vendors from claims arising from data breaches has nothing to do with the congressional intent underlying the ADA.

26. The ADA is based on the view that the best interests of airline passengers are most effectively promoted, in the main, by allowing the free market to operate. Invocation of the ADA in the data breach context, however, turns the ADA on its head. The evolving state of data privacy was the topic of an address by FTC Commissioner Julie Brill. In her address, Commissioner Brill noted that

the Notice and Choice approach has become the primary online privacy protection mechanism. Disclosure through Notice and Choice encourages privacy-based competition. With proper notice, individuals can compare services based on their stated information practices and can choose to transact with services based on how those practices comport with the individual's privacy preferences.[10] Competition regarding privacy notices is needed to incentivize companies to provide better protection to their customers. Immunizing companies such as Defendants from lawsuits obviates any incentive to engage in such competition. Furthermore, any assertion that an airline privacy policy is merely an illusory promise undermines the Notice and Choice approach.

B. The Breach

27. On April 5, 2018, Delta disclosed on its website that between September 26 and October 12, 2017, [24]7.ai, a chat service retained by Delta to communicate with customers on its website, had experienced a malware attack that exposed highly confidential information belonging to hundreds of thousands of Delta customers to theft and misuse by persons or entities with malicious intent. The exposed information includes credit and debit card account numbers, card verification codes, and expiration dates, as well as full names, mailing addresses, and potentially other information.

28. On or about April 11, 2018, Delta sent a letter to Plaintiff and other affected customers disclosing this breach. Delta did not send this letter to its customers until approximately six months after the breach occurred, and until nearly two weeks after Delta stated it learned of it from [24]7.ai.

29. Delta set up a webpage concerning this breach. The page is scant in the detail that it provides as to how the breach occurred or why it took so long to disclose it to consumers, but does provide the following information:

[10] *Proskauer on Privacy*, Remarks by FTC Comm. Julie Brill, Oct. 10, 2010.

30. It explains what [24]7.ai is: "[24]7.ai is a company that provides online chat services for many companies, including Delta."[11]

31. It also states that, **"Customers did not have to interact with the online chat tool to be impacted"** by the data breach. (Emphasis supplied.) The website offers no explanation as to why Delta provided confidential Customer Data to a chat service provider when those customers did not use that chat service.[12]

32. The website also sets forth Delta's claims as to the timeline of the breach and disclosures. It states that Defendant [24]7.ai "became aware of the cyber incident on October 12, 2017." Delta claims to have learned about the breach on March 28, 2018 (Plaintiff does not concede that Delta did not learn of the breach until this date), but it took Delta still another week, until April 5, 2018, to set up a website at last making public disclosure of the issue, and nearly a week beyond that to send out a letter to customers.[13]

33. The excessive delay in disclosing the breach is even more clear with respect to Defendant [24]7.ai. According to Delta, [24]7.ai took steps to implement a fix for the malware on October 12, 2017. [24]7.ai must, thus, have known about the breach at that time. If [24]7.ai did not, as Delta claims, inform Delta of the breach until March 28, 2018, it left Plaintiff and the other Class members needlessly and unknowingly exposed to risk, and thus unable to take steps to even attempt to protect to themselves, for six months.[14]

C. [24]7.ai's Services

34. [24]7.ai describes its chat services as "delivering significant support cost reduction [to [24]7.ai's clients like Delta] and sales revenue uplift by

[11] https://www.delta.com/content/www/en_US/response.html (last visited Jan. 21, 2019)
[12] *Id.*
[13] *Id.*
[14] *Id.*

deflecting contacts from phone and email."[15] This is not a service that is inherently related to the price, route or service of an air carrier, but instead, is an alternate means of communication that can be used by any company. Indeed, in the same Data Breach that impacted Delta customers, [24]7.ai also exposed the data of customers of other companies including non-airlines Best Buy and Sears. Internet chat services do not impact the prices, schedules, origins or destinations of the point-to-point transportation of airline passengers, cargo, or mail. An internet chat service is at most, akin to a kiosk operated by an airline at an airport to facilitate ticketing and the provision of information to consumers, or to a toll free service provided by an airline to facilitate the purchase of tickets.

35. This lack of connection to air carrier services is true of both [24]7.ai's services themselves and Delta's decision to make use of those services, and actions in connection therewith.

D. Defendants' Obligations

36. In recent years, attempted data breaches have become a basic and foreseeable risk that must be protected against by any company that enables customers to provide personal information on their website. Delta, a major airline that conducts extensive business through its website, was at all times aware of this and obligated to take appropriate precautions, including, but not limited to, protecting against breaches, protecting Customer Data and monitoring [24]7.ai such that it would discover and/or be notified of any data breaches in a timely manner. [24]7.ai, a company whose primary business is the use of information provided by consumers over the internet, similarly knew of these dangers and was obligated to provide adequate internet security and timely notice to customers of any data breach.

[15] https://www.247.ai/customer-engagement/247-chat (last visited January 21, 2019).

37. Delta obtains a great deal of sensitive customer information through its website. This information includes credit and debit card account information, security codes, contact addresses, and other information that is extremely valuable to malicious agents who seek to use it for their profit at the expense of the information's actual owners.

38. Delta's obligations to its customers are set forth in an integrated contract that includes Delta's Privacy Policy, the Contract of Carriage and ticket issued to customers.

E. Delta's Privacy Policy

39. Delta's Privacy Policy constitutes an agreement between Delta and those individuals who provided personal information to it, including Plaintiff and the Class. As stated below, [24]7.ai agreed to be bound by Delta's Privacy Policy and is bound by its terms. A full copy of Delta's Privacy Policy is attached hereto at Exhibit A.

40. The Contract of Carriage states that the terms of the contract are set forth in, among other things, "your ticket." Plaintiff's ticket receipt states: "Your privacy is important to us. Please review our Privacy Policy." A copy of Plaintiff's ticket receipt is attached hereto at Exhibit B.

41. In the Privacy Policy, Delta expressly acknowledges its duty to safeguard Customer Data. Its Privacy Policy states, and has stated at all relevant times:

> Information Security is important to Delta. We have established appropriate physical, electronic and managerial safeguards to protect the information we collect from or about our users. These safeguards are regularly reviewed to protect against unauthorized access, disclosure and improper use of your information, and to maintain the accuracy and integrity of that data.

42. Delta and [24]7.ai breached the Privacy Policy contained in the contract by failing to establish appropriate physical, electronic and managerial safeguards to protect Customer Data, by failing to regularly review the safeguards and by failing to take steps to protect the Customer Data of Plaintiff and the Class.

43. Delta had an obligation to oversee [24]7.ai and ensure that its data security provisions met Delta's standards. Delta's failure to identify the flaws in [24]7.ai's data security provisions and failure to detect the breach for over six months shows disregard for the safety of Customer Data, and constitutes a breach of the Privacy Policy that is a part of its contract with its customers.

44. Likewise, [24]7.ai breached the Privacy Policy by allowing hackers to access Customer Data for two weeks before detecting the malware. Both Defendants failed to regularly review safeguards and protect against unauthorized access, disclosure and improper use of Customer Data.

45. The Privacy Policy also states:

> "We do not sell your name or other personally identifiable information to third parties, and do not intend to do so in the future. We routinely share your information with our SkyMiles Partners and Promotional Partners and our subsidiaries including Delta Connection® Carriers. From time to time, we may engage third parties to process your information on our behalf, or to assist us in improving our services and/or products; however, **Delta requires that these third parties comply with Delta's Privacy Policy when processing your information**. When you purchase services or products through Delta that are to be provided by another party (for example, a travel segment on another carrier, hotel accommodations, or rental car), we share your information with the third-party so that the third-

> party can provide the services or products you requested. We may also receive information about you from the third-party providers. We may share with third parties anonymous, aggregated information about all our users. From time to time, Delta may combine information we collect from you with information that we receive from third parties or collect from other sources. We may use this information to provide offers specifically tailored to your interests." (emphasis added).

46. Although the Privacy Policy states, on its face, that it is not a contract, it creates reasonable expectations on the part of Delta customers and thus induces them to disclose their confidential information and purchase tickets. This gives rise to a contractual relationship. Delta may not use the Privacy Policy to induce customers to provide Customer Data but, then only abide by the terms of the Privacy Policy when it wants to.

47. Moreover, the Privacy Policy states that Delta "requires that…third parties [like [24]7.ai] comply with Delta's Privacy Policy when processing [Customer Data]." Plaintiff and other Class Members are third party beneficiaries of any contract between Delta and [24]7.ai requiring [24]7.ai to comply with Delta's Privacy Policy.

48. [24]7.ai also acknowledges its obligations with respect to the Consumer Data of its clients like Delta. Its website states:

> Security is a big concern for organizations looking to adopt the cloud. We continually implement robust technical and organizational security controls to ensure customer data is safe.[16]

[16] https://www.247.ai/security

49. Upon information and belief, airlines have represented to the Department of Transportation that they follow their privacy policies. Accordingly, it would be unconscionable and Defendants would be estopped under the theory of Promissory Estoppel from asserting that Delta's Privacy Policy is not an express term of the contract with Plaintiff and the Class members.

F. Contract of Carriage

50. In addition to the Privacy Policy, which is part of the contract between Delta and its customers, Delta also required all consumers purchasing tickets through its website to be party to its Contract of Carriage, which also contained protections for Customer Data. The Contract of Carriage provides:

> **RULE 25: PERSONAL DATA**
>
> The passenger recognizes that personal data has been given to carrier for the purposes of making a reservation for carriage, obtaining ancillary services, facilitating immigration and entry requirements, and making available such data to government agencies. For these purposes, the passenger authorizes carrier to retain such data and to transmit it to its own offices, other carriers, or the providers of such services, in whatever country they may be located.

51. The terms of the Contract of Carriage, at the very least, would not authorize Delta to "transmit" Plaintiff's and Class Members' Customer Data to any third parties after the date when due diligence would have revealed inadequate safeguards by the third party of Customer Data and/or from the date that the Data Breach had occurred.

52. By sharing Plaintiff's and Class members' Customer Data with [24]7.ai, Delta breached the Contract of Carriage with Plaintiff and Class members.

G. [24]7.ai's Contract with Delta

53. Delta and [24]7.ai entered into a Subscription Services Agreement dated July 24, 2017 ("Agreement") for a term of three years. The Agreement contains multiple promises about the protection of Class members' PII for the

intended benefit of the Class. The Agreement makes clear that Plaintiff and Class members are intended third party beneficiaries of the Agreement.

54. For example, the Agreement has an entire addendum titled Exhibit C, "Personally Identifying Information," which sets forth in detail the things 24[7].ai was contractually required to do to protect the data that was stolen from Class Members. It defines "Personally Identifying Information" or "PII" as including "any information regarding identifiable individuals, including without limitation, customer, employee or member data." It states, as a general principle, that the "Service Provider agrees to use reasonable measures to prevent the unauthorized processing, capture, transmission and use of PII which may be disclosed or made available to Service Provider during the course of Delta's relationship with Service Provider." Agreement, Exhibit C, at (a).

55. Exhibit C states that the "Service Provider" ([24]7.ai) was required to take steps including the following:

> (i) Access of Persons: Service Provider agrees to use reasonable measures, including encryption, to prevent unauthorized persons from gaining access to the data processing equipment or media where PII is stored or processed. Service Provider agrees to provide its employees and agents access to PII on a need-to-know basis only and agrees to cause any persons having authorized access to such information to be bound by obligations of confidentiality, non-use and non-disclosure ….
>
> (ii) Data Media: Service Provider agrees to use reasonable measures, including encryption, to prevent the unauthorized reading, copying alteration or removal of the data media used by Service Provider and containing PII.

> (iii) Retention: Service Provider shall not retain PII any longer than is reasonably necessary to accomplish the intended purposes for which PII was transferred as set forth in this Agreement.…
>
> (iv) Data Memory: Service Provider agrees to use reasonable measures, including encryption, to prevent unauthorized data input into memory and the unauthorized reading … of PII.
>
> (vi) Transmission: Service Provider agrees to use reasonable measures, including encryption, to prevent PII from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media on which PII is stored.
>
> …
>
> (g)… report security breaches (data or network) to Delta in a prompt and timely manner and assist Delta's Information Security and Privacy Office ("ISPO") in the investigation thereof.

56. The foregoing provisions in Exhibit C were expressly intended to benefit Delta's customers, including Plaintiff and the Class. Defendants breached these provisions by failing to take the required actions to secure the Customer Data, permitting hackers to access Plaintiff and the Class members' Customer Data and failing to provide timely notification of the breach.

57. The Agreement has another addendum, Exhibit D, "Electronic Access." Exhibit D states that the "Service Provider shall not permit or allow any unauthorized person or third party to access, use or modify the Permitted Systems," which is defined to include "Confidential Information, Personally Identifying Information and related computer systems and files that Delta expressly authorizes it to access, use, or modify." These obligations too were for the intended benefit of Plaintiff and the Class.

58. Defendants breached this provision by permitting unauthorized access to Plaintiff and the Class members' Customer Data.

59. The Agreement also includes a warranty for the express intended benefit of Delta's customers:

> Service Provider shall take commercially reasonable efforts to avoid the introduction, and Service Provider will not subsequently introduce into the Subscription Services, the Software or the Customer Data, any 'back door,' 'time bomb,' 'Trojan horse,' 'worm,' 'drop dead device,' 'virus,' 'preventative routines' or other computer software routines designed: to permit access to or use of Delta's computer systems by Service Provider or a third party not authorized by this Agreement; to disable, modify, damage or delete the Customer Data and any data, software, computer hardware or other equipment operated or maintained by Delta; or to perform any other such similar actions.

Agreement at §8.2; *see also* Exhibit D, "Electronic Access" paragraph (e).

60. Defendants breached this provision by permitting hackers to access Defendants' computer systems and steal Customer Data.

61. The Agreement also represents that the Service Provider shall comply with Payment Card Industry Data Security Standards:

> Service Provider shall (a) comply with, and shall have a program to assure its continued compliance with, the Payment Card Industry Data Security Standards (the "PCI DSS") published by the PCI Security Standards Council, as the PCI DSS may be amended, supplemented, or replaced from time to time; (b) provide proof of its PCI DSS compliance in writing to Delta at least once each year; and (c) promptly report in writing to Delta if Service Provider becomes aware that it is not, or will not likely be, in compliance with PCI DSS for any reason.

Agreement at §3.7

62. Upon information and belief Defendants did not comply with PCI DSS.

63. The PCI DSS includes numerous provisions applicable to the Class, which, if Defendants had adequately followed, would have prevented or minimized injury to the Class.

64. For example, Section 10.6.1 includes the following standard:

> Checking logs daily minimizes the amount of time and exposure of a potential breach.
>
> Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential

issues.

65. It thus includes this requirement:

> 10.6.1 Review the following at least daily:
>
> · All security events
>
> · Logs of all system components that store, process, or transmit CHD and/or SAD
>
> · Logs of all critical system components
>
> · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

66. If Defendants had reviewed all security events daily as required, the Data Breach may not have occurred at all, or, if it did, the Data Breach would have been discovered sooner than it reportedly was, and the damage to the Class would have been limited.

67. Similarly, Section 11.4 includes the following requirement:

> 11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

68. If Defendants had monitored such vulnerability points on an ongoing basis, the Data Breach may not have happened or Defendants would have caught the breach when it happened.

69. In short, if Defendants had fulfilled their obligations under these and other requirements of the PCI DSS, the Class would not have been injured or its harm would have been limited

70. The contract provisions, including Exhibit C, Exhibit D and the obligation to comply with PCI DSS, make clear that Plaintiff and Class members are express intended third party beneficiaries of the Agreement. While there is a provision in the main body of the Agreement that includes the boilerplate language that "No third party is intended to benefit from, nor may any third party seek to enforce, any of the terms of this Agreement," Agreement 15.7, Section 15.11 of the Agreement, states that "Every exhibit and attachment to this Agreement is an integral part of this Agreement and is incorporated into this Agreement … Should any term contained in any exhibit or attachment conflict with any provision of this Agreement, the provision contained in the exhibit or attachment controls, unless the term contained in this Agreement expressly states otherwise." The Exhibits to the Agreement, including, most obviously Exhibit C, clearly are for the express intended benefit of Plaintiff and Class members and, consequently, trump the boilerplate "no third party beneficiary" provision in the Agreement.

71. Delta's Privacy Policy in effect at the time of the breach stated that it may "engage third parties to process your information on our behalf or to assist us in improving our services and/or products; however Delta ***requires that these third parties comply with Delta's Privacy Policy when processing your information***." (Emphasis supplied.)

72. Moreover, [24]7.ai's own privacy policy not only concedes how much information it collects, but indicates that it does so at the "contractual direction" of clients such as Delta. [24]7.ai's privacy policy states:

> At the contractual direction of [24]7.ai's clients, [24]7.ai collects and processes End User's information which may include Personal Information, where "Personal Information" means information that can be used to specifically identify an End User, including, but not limited to, a first and last name, organization name, email address, phone number, postal/zip or

> other physical address, date of birth, gender, professional title, account information, credit/debit card number, and any other such information needed by the [24]7.ai Platform to provide client-specified services to an End User. [24]7.ai respects the privacy of End Users and is committed to protecting the Personal Information that we receive through their direct and indirect use of the [24]7.ai Platform. Notwithstanding the foregoing, End Users' use of our clients' Internet- and telephony- based services (and, ultimately, the [24]7.ai Platform) is solely governed by the terms and conditions agreed to directly between End Users and [24]7.ai's clients (usually via a signed written agreement, "Terms of Use" and/or a "Privacy Policy" on such clients' websites).[17]

73. Although the above policy indicates that end users' use of Delta's platform, and [24]7.ai's platform is governed by terms and conditions agreed to between Delta and the end users, that does not eliminate [24]7.ai's obligation to take reasonable measures to protect the end users' information that it obtains.

74. Plaintiff and other Class members are express intended third party beneficiaries of the Agreement and any other contract between Delta and [24]7.ai in which [24]7.ai promises to protect the Customer Data of users of Delta's website.

H. Defendants' Security Protocols Were Insufficient

75. Delta and [24]7.ai maintained an insufficient and inadequate system to protect the Customer Data of Plaintiff and the Class. It is well known, and the subject of many media reports, that Customer Data is highly coveted and a

[17] https://www.247.ai/privacy-policy#platform-policy (visited January 21, 2019).

frequent target of hackers. Despite well-publicized litigation and frequent public announcements of data breaches, Defendants maintained an insufficient and inadequate system to protect the Customer Data of Plaintiff and the Class.

76. There have been a number of recent high profile data breaches. Breaches at entities such as Equifax, Yahoo, Facebook, Apple, Target, Ebay, Anthem, Home Depot, United States Office of Personnel Management, and UCLA Health System, to name a few, have garnered national attention. As a result of the increasing amount of data breaches involving vast quantities of Customer Data, Defendants were on notice that they needed to take precautions to prevent something similar from happening to the Customer Data they collected over the Internet.

77. The exposure of Plaintiff's and the Class's Customer Data to unauthorized third party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and the Class's Customer Data from unauthorized access, use, and disclosure as well as Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class's Customer Data in order to protect such data against reasonably foreseeable threats to the security of such information.

78. Defendant [24]7.ai knew or should have known that its data security protocols were inadequate and vulnerable to being breached by hackers. Had Defendants implemented such adequate and reasonable security measures, Plaintiff and the other Class members would not have suffered the injuries alleged, as the Data Breach would likely not have occurred.

79. Plaintiff would not have used her payment card or otherwise provided personal data on Delta's website to make a purchase had Plaintiff known that Delta and [24]7.ai, whose involvement Plaintiff and the Class were not aware, lacked adequate computer systems and data security practices to safeguard Customer Data

from theft. Indeed, Plaintiff would not have patronized Delta at all during the period of the data breach and, thus, she suffered actual injury and damages in paying money for the purchase of air travel from Delta that she would not have paid had [24]7.ai and Delta made such disclosures.

80. Plaintiff would not have authorized [24]7.ai to access her information if it were known that [24]7.ai's security measures were inadequate, and most certainly would not authorize such access after the Data Breach occurred.

I. Delta's letter to Plaintiff

81. In April 2018, Plaintiff received a letter from Delta notifying her of the Data Breach. The letter stated:

> We are writing to tell you about a cyber incident involving [24]7.ai, a company that provides online chat services for Delta and many other companies. This incident may have resulted in unauthorized access to payment card information relating to a purchase you made on delta.com. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take very seriously. We've included in this letter the information we have on the incident as well as instructions to contact the team dedicated to answering your questions should you need additional assistance.
>
> We cannot at this point say definitively whether any of our customers' information was accessed. However, out of an abundance of caution and as part of our commitment to the security of your information, we are partnering with AllClear ID, a leading customer security and fraud protection firm, to offer a suite of identity theft protection and credit monitoring

services for two years from the date of this letter at no cost to you. As an eligible customer, you can enroll in this service by calling (855) 815-0534 or visiting delta.allclearid.com.

The latest updates on this incident will be available at delta.com/response.

What Happened

On March 28, 2018, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 26 to Oct. 12, 2017 and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed – no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.

We understand malware present in [24]7.ai's software between Sept. 26 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CVV number, and expiration date. There was no impact to the Fly Delta app, mobile delta.com or and Delta computer system.

At this point, even though only a small subset of our customers

would have been exposed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.

Based on our investigation to date, we have determined that the payment card information of customers who completed a purchase on the delta.com desktop platform between Sept. 26, 2017 and Oct. 12, 2017 may have been exposed. Our records indicate that you may have completed such a purchase during this time frame. As a result, information relating to the payment card used for that purchase may have been exposed, including name, address, payment card number, CVV number, and expiration date. No other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.

What We Are Doing

While [24]7.ai recently advised us that the incident was contained and stopped on Oct. 12, 2017, upon learning of the incident, Delta immediately launched an investigation and engaged federal law enforcement and forensic teams. We have also initiated diligent efforts to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber event.

Delta is committed to protecting your personal information and, out of an abundance of caution, is offering you a paid

> subscription for AllClear ID credit monitoring and identity theft protection services for two years at no cost to you. Information on how to enroll in these services is included with this notice.
>
> The latest information will be available to you at delta.com/response.
>
> *Excerpt from the Letter from Delta to Plaintiff dated April 11, 2018, attached hereto as Exhibit C.*

J. Defendants' Conduct Following the Breach

82. Defendants' conduct following the breach only compounded the injury to Plaintiff and the Class. Despite the hack occurring six months prior, and [24]7.ai's clear knowledge of the breach six month prior given that that is when it took remedies to address the malware, Delta customers were not notified of the breach of their sensitive information until April 2018. Their Customer Data was available to hackers for six months without their knowledge, and even for nearly two weeks after Delta acknowledged that it knew of the breach. Data thieves had use of the Customer Data during this time while Delta customers were totally unaware and thus they could take no action to protect themselves.

83. Delta had an obligation to oversee the data security provisions used by [24]7.ai. Delta's failure to detect the breach or identify the weakness in [24]7.ai's security protocols indicates a failure of oversight. Delta should have had a team devoted to maintaining the security of Customer Data that should have identified flaws in [24]7.ai's protocols and identified the breach as soon as it occurred. Instead, Delta had to be notified by [24]7.ai of the breach six months after it occurred. That Delta claims it was not aware of the breach until March 2018 indicates a lack of communication between Delta and [24]7.ai and a total lack of

oversight by Delta.

84. Delta's lack of care concerning this breach is further evidenced by the status of the website it set up for customers to visit for updated information on the Data Breach.[18] On the website Delta states: "The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take extremely seriously." However, the website was last updated on April 7, 2018. Delta stated that it "launched an investigation and engaged federal law enforcement and forensic teams." Plaintiff and the Class have not been updated on the status or results of those investigations or anything else relating to the breach.

85. Through their failure to timely discover and provide clear notification of the Data Breach to consumers, Defendants prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their Customer Data.

K. Plaintiff and the Class Suffered Damages

86. The data breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class's Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law. The data breach was also a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class's Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

87. Delta's own Privacy Policy falsely states that "[Delta has] established appropriate physical, electronic and managerial safeguards to protect the information we collect from or about our users."

88. Defendants had the resources to prevent a breach. This is especially

[18] https://news.delta.com/updated-statement-247ai-cyber-incident. Last accessed January 10, 2019.

true for [24]7.ai as it is in the data collection business and given its partnerships with Sequoia Capital and Microsoft. However, despite these available resources, Defendants maintained inadequate safeguards, capable of being accessed by hackers. Delta customers were not the only ones affected by the Data Breach. The Customer Data of other [24]7.ai clients including Best Buy and Sears was also stolen by hackers.

89. Had Defendants employed security measures recommended by experts in the field, Defendants would have prevented intrusion into their computer systems and, ultimately, the theft of their customers' Customer Data.

90. Plaintiff's and the Class's Customer Data is their property, it is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiff's and Class's consent to disclose their Customer Data as required by applicable law and industry standards.

91. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. [24]7.ai has not offered any identity protection to affected customers. Delta has stated that it is offering its customers affected by the Data Breach two years of identity protection services, but credit monitoring services alone, especially for such a limited period of time, are insufficient. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

92. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Customer Data—personal property that she entrusted to Delta (and which Delta gave to [24]7.ai without her knowledge) as a form of payment that was compromised as a result of the Data Breach.

93. Plaintiff further suffered actual injury in the form of time spent investigating fraud resulting from the Data Breach, paying for third party

monitoring, and monitoring her accounts for additional fraud.

94. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Customer Data being placed in the hands of criminals who would not have stolen the data if they did not intend to use it for fraud. Even though Plaintiff cancelled the credit card she used when using the Delta website after receiving notice of the Data Breach, Plaintiff's newly issued credit cards have reflected unauthorized charges on two occasions since then.

95. The violation is ongoing because [24]7.ai is still accessing Customer Data of Plaintiff and members of the Class. Plaintiff has a continuing interest in ensuring that her private property and information, which remains in the possession of [24]7.ai and Delta, is protected and safeguarded from future breaches. Moreover, the Customer Data should be deleted and cookies removed.

96. As a direct and proximate result of Defendants' wrongful action and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

97. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class's Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Theft of their Customer Data;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their Customer Data being placed in the hands of criminals;

c. The imminent and impending injury flowing from sale of Plaintiff's and the Class Members' Customer Data on the Internet black market;

d. The untimely and inadequate notification of the data breach;

e. The improper disclosure of their Customer Data;

f. Loss of privacy;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of their Customer Data, for which there is a well-established national and international market;

i. Overpayments to Defendants for booking and purchase during the subject data breach in that a portion of the price paid for such booking by Plaintiff and Class to Defendants was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Customer Data, which Defendants did not implement and, as a result, Plaintiff and

Class did not receive what they paid for and were overcharged by Delta, and by [24]7.ai to the extent that [24]7.ai's charges were passed along by Delta to customers;

j. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

k. Deprivation of rights they possess under the Unfair Competition Laws.

98. While Plaintiff's and the Class's Customer Data has been stolen, Defendants continue to hold Customer Data of consumers, including Plaintiff and the Class members. Particularly because Defendants have demonstrated an inability to prevent a breach, Plaintiff and the Class members have an undeniable current interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

V. CLASS ACTION ALLEGATIONS

99. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts that Defendants are liable for common law claims for breach of contract (and third party beneficiary of contract), bailment, unjust enrichment, as well as violations of statutory law. Plaintiff and the members of the Class are

entitled to declaratory and injunctive relief, on behalf of the following nationwide class (the "Nationwide Class" or the "Class"):

> All persons residing in the United States who made a reservation on Delta's website from the time period September 26, 2017 to October 12, 2017 (the "Nationwide Class").

100. The (the "State Name Class") is initially defined as follows:

> All persons residing in (State Name) who made a reservation on Delta's website from the time period September 26, 2017 to October 12, 2017 (the "State Name Class").

101. Excluded from each of the above Classes are Defendants, including any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

102. **Numerosity.** Fed. R. Civ. P. 23(a)(1). The members of the Classes are so numerous that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, Defendants have estimated that the number is in the hundreds of thousands. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as reservation receipts and confirmations.

103. **Commonality and Predominance.** Fed. R. Civ. P. 23(a)(2) and

(b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class's Customer Data;

b. Whether Defendants knew or should have known of the susceptibility of their computer systems to a data breach;

c. Whether Defendants willfully or recklessly failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Customer Data;

d. Whether Plaintiff's and the Class members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

e. Whether Defendants violated common and statutory law by failing to promptly notify the Class that their Customer Data had been compromised;

f. Whether Defendants breached their contractual obligations owed to Plaintiff and the Class by failure to use reasonable security measures;

g. Whether Defendants breached their contractual obligations owed to Plaintiff and the Class by failure to timely notify the

Class of the Data Breach;

h. Which security procedures and which data-breach notification procedure should Defendants be required to implement as part of any injunctive relief ordered by the Court;

i. Whether Defendants knew or should have known of the security breach prior to the disclosure;

j. What security measures, if any, must be implemented by Defendants to comply with their contractual obligations;

k. What the nature of the relief should be, including equitable relief, to which Plaintiff and the Class are entitled; and

l. Whether Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

104. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved and common questions of law and fact predominate.

105. **Typicality.** Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of the Class because Plaintiff's Customer Data, like that of every other Class Member, was stolen through a malware attack. Plaintiff and the Class were injured through Defendants' substantially uniform misconduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and Class members and there

are no defenses that are unique to Plaintiff's claims. Plaintiff and the Class's claims arise from the same operative facts and are based on the same legal theories.

106. **Adequacy of Representation.** Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained competent counsel experienced in litigation of complex class actions, including consumer and data breach class actions, and Plaintiff intends to prosecute this action vigorously. Plaintiff's claims are typical of the claims of other members of the Class and Plaintiff has the same non-conflicting interests as the Class. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

107. **Superiority of Class Action.** Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class and Subclass members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for the Class members to individually seek redress for Defendants' wrongful conduct. Even if the Class members could afford individual litigation, individual litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

108. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding

declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COUNT I

Breach of Contract Against Delta and [24]7.ai

On behalf of Plaintiff and the Class as Third-Party Beneficiaries[19]

109. Plaintiff, individually and on behalf of all other Class members, alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 108, inclusive of this Amended Complaint as if set forth fully herein.

110. The Agreement is a valid and enforceable express contract between Delta and 24[7].ai for the express intended benefit of Delta's customers. Under the Agreement, Delta gave [24]7.ai access to its Customer Data, [24]7.ai provided online chat services on Delta's website, and Delta compensated [24]7.ai for its services.

111. As detailed in Exhibits C and D of the Agreement, Defendants agreed to take measures to keep Plaintiff and the Class members' Customer Data secure.

112. Defendants breached the Agreement by failing to take appropriate steps to secure Customer Data and permitting hackers to access Customer Data.

113. Under Exhibit C and § 3.7 of the Agreement Defendants also agreed to provide timely notice of a breach.

114. Defendants breached the Agreement by failing to provide notice of the Data Breach until more than six months after the Data Breach occurred.

[19] In its Order dated April 16, 2019, the Court denied Plaintiff's Motion for Leave to File Amended Class Action Complaint with respect to the claims for negligence, violation of state consumer protection statutes and violation of state data breach acts. Plaintiffs reserves her right to appeal the denial of her motion to assert these claims.

115. Under the Agreement Defendants agreed to comply with Payment Card Industry Data Security Standards ("PCI DSS").

116. Defendants breached the Agreement by failing to comply with the PCI DSS and failing to provide timely notice of the breach.

117. Delta's Privacy Policy states that Delta had in place appropriate physical, electronic and managerial safeguards to protect the information it collects from the end users of its website, and that the safeguards are regularly reviewed to protect against unauthorized access, disclosure and improper use of its customers' information, and to maintain the accuracy and integrity of that data.

118. Delta's Privacy Policy further states that it may engage third parties to process its customers' information on its behalf, or to assist it in improving its services and/or products, and that Delta requires these third parties to comply with Delta's Privacy Policy when processing its customers' information.

119. Delta engaged [24]7.ai, a third party, to provide online chat services on Delta's website for the benefit of its customers. As such, under its Contract with [24]7.ai, Delta required [24]7.ai to comply with Delta's Privacy Policy when processing Delta's customers' information.

120. [24]7.ai's privacy policy states that "[a]t the contractual direction of [24]7.ai's clients," like Delta, "[24]7.ai collects and processes End User's information which may include Personal Information, where "Personal Information" means information that can be used to specifically identify an End User, including, but not limited to, a first and last name, organization name, email address, phone number, postal/zip or other physical address, date of birth, gender, professional title, account information, credit/debit card number, and any other such information needed by the [24]7.ai Platform to provide client-specified services to an End User."

121. [24]7.ai's privacy policy also states that "[24]7.ai respects the privacy of End Users and is committed to protecting the Personal Information that we

receive through their direct and indirect use of the [24]7.ai Platform," and that "End Users' use of our clients' Internet- and telephony- based services (and, ultimately, the [24]7.ai Platform) is solely governed by the terms and conditions agreed to directly between End Users and [24]7.ai's clients (usually via a signed written agreement, "Terms of Use" and/or a "Privacy Policy" on such clients' websites)."

122. [24]7.ai also states on its website that, because security of customer data is a big concern for [24]7.ai, it continually implements robust technical and organization security controls to ensure customer data is safe.

123. While Plaintiff and the Class are not parties to the Agreement, given the purpose of and the services to be provided under the Agreement, and the surrounding circumstances, including Delta's and [24.7].ai's public statements about their duties to protect Customer Data, Plaintiff and the Class are intended third party beneficiaries of the Agreement.

124. The benefits that Plaintiff and the Class were to receive as intended third party beneficiaries of the Agreement were not incidental to the Agreement.

125. [24]7.ai breached the Agreement by failing to adequately safeguard Plaintiff's Customer Data. In breach of its contractual promise, [24]7.ai did not comply with Delta's Privacy Policy for the intended benefit of Plaintiff and the Class.

126. [24]7.ai also breached the Agreement by failing to inform Delta in a timely manner of the malware attack that exposed Delta's customers' Customer Data to thieves and put the Customer Data of Plaintiff and the Class at risk.

127. Upon information and belief, [24]7.ai also breached the Agreement by failing to continually implement robust technical and organization security controls to ensure Delta's customers Customer Data was and remained safe.

128. Delta, in turn, breached the Agreement by failing to monitor [24]7.ai to ensure its compliance with Delta's Privacy Policy and other provisions in the

Agreement to protect the Customer Data of its customers, and by failing to enforce the Agreement.

129. As a direct and proximate result of Delta's and [24]7.ai's breaches of the Agreement, Plaintiff and the Class, as express intended third party beneficiaries of the Agreement, sustained actual losses and damages as described in detail above in an amount to be proven at trial.

COUNT II

Breach of Contract Against Delta

130. Plaintiff, individually and on behalf of all other Class members, alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 129, inclusive of this Amended Complaint as if set forth fully herein.

131. Delta solicited and invited Plaintiff and the members of the Class to make flight and/or other travel related reservations with Delta. Plaintiff and Class members accepted Delta's offer and made such reservations with Delta. Delta's Privacy Policy and Contract of Carriage constitute part of the contract with Plaintiff and members of the Class.

A. Privacy Policy

132. Delta's Privacy Policy induced customers to provide their Customer Data to Delta and purchase tickets over the Delta website.

133. Delta breached the Privacy Policy.

134. In its Privacy Policy, Delta represented that it "established appropriate physical, electronic and managerial safeguards to protect the information we collect from or about our users. These safeguards are regularly reviewed to protect against unauthorized access, disclosure and improper use of your information, and to maintain the accuracy and integrity of that data."

135. Plaintiff and Class members would not have provided and entrusted their Customer Data to Delta if Plaintiff knew that Delta would not safeguard and protect Customer Data and regularly review its protocols to ensure that Customer Data was protected.

136. Plaintiff and Class members fully performed their obligations under the contract with Defendants.

137. Delta breached the Privacy Policy contained in the contract it made with Plaintiff and Class members by failing to adequately monitor [24]7.ai, failing to safeguard and protect the Customer Data from unauthorized access, disclosure and improper use and by failing to provide timely and accurate notice to Plaintiff and the Class that their Customer Data was compromised as a result of the Data Breach.

B. Contract of Carriage

138. Delta's Contract of Carriage is an agreement between Delta, on one hand, and Plaintiff and Class members, on the other hand, who have made a booking with Delta and, in the process of doing so, provided their Customer Data to Delta.

139. The Contract of Carriage, at the very least, would not authorize Delta to "transmit" Plaintiff's and Class Members' Customer Data to any third parties after the date when due diligence would have revealed inadequate safeguards of Customer Data and/or from the date that the data breach had occurred.

140. In breach of the terms of the Contract of Carriage, Delta transmitted and/or shared the Customer Data of Plaintiff and Class members with [24]7.ai after the date when due diligence would have led to the discovery of the flaws in 24[7].ai's data protection systems, and even after the Data Breach occurred.

141. Plaintiff and Class members fully performed their obligations under the Contract of Carriage with Delta.

142. As a direct and proximate result of Delta's breach of the Contract of Carriage and Privacy Policy and the ensuing Data Breach, Plaintiff and Class members sustained actual losses and damages as described in detail above. Plaintiff and Class members have been placed at an imminent, immediate, and continuing risk of identity theft-related harm and are thereby entitled to recover compensatory damages in an amount according to proof at trial.

COUNT III

Unjust Enrichment Against Delta

143. Plaintiff, individually and on behalf of all other Class members, alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 142, inclusive of this Amended Complaint as if set forth fully herein.

144. Defendant Delta has been unjustly enriched at the expense of Plaintiff and members of the Class.

145. Plaintiff and the Class members conferred a monetary benefit on Delta.

146. Delta failed to secure Plaintiff and the Class members' Customer Data and, therefore, did not provide full benefits for which Plaintiff and the Class members paid.

147. Plaintiff and the Class members have no adequate remedy at law.

148. Under the circumstances, it would be unjust for Delta to be permitted to retain any of the benefits that Plaintiff and the Class members conferred.

149. Delta should be compelled to disgorge the proceeds Delta unjustly received from Plaintiff and the Class members. In the alternative, Delta should be compelled to refund the amounts that Plaintiff and the Class members overpaid.

COUNT IV

Bailment Against Delta

150. Plaintiff, individually and on behalf of all other Class members, alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 149, inclusive of this Amended Complaint as if set forth fully herein.

151. Plaintiff and the other Class members provided, or authorized disclosure of, their Property, that is, their Customer Data to Delta.

152. In allowing their Customer Data to be made available to Delta, Plaintiff and the other Class members intended and understood that Delta would adequately safeguard their Customer Data.

153. Delta accepted possession of Plaintiff's and the other Class members' Customer Data.

154. By accepting possession of Plaintiff's and the other Class members' Customer Data, Delta understood that Plaintiff and the other Class members expected Delta to adequately safeguard their Customer Data. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Delta owed a duty to Plaintiff and the other Class members to exercise reasonable care, diligence, and prudence in protecting their Customer Data.

155. Delta breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and the other Class members' Property, that is, their Customer Data, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and the other Class members' Customer Data.

156. Delta further breached its duty to safeguard Plaintiffs' and the other Class members' Customer Data by failing to timely and accurately notify them that their information had been compromised as a result of the Data Breach.

157. As a direct and proximate result of Delta's breach of its duty, Plaintiff and the other Class members suffered damages that were reasonably foreseeable to

Delta, including but not limited to the damages set forth above.

158. As a direct and proximate result of Delta's breach of its duty, the Property, that is, Customer Data, of Plaintiff and the other Class members entrusted, directly or indirectly, to Delta during the bailment (or deposit) was damaged and its value diminished.

COUNT V

Violation of the Federal Stored Communications Act,

18 U.S.C. §§ 2701 *et seq.* Against [24]7.ai

159. Plaintiff, individually and on behalf of all other Class members, alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 158, inclusive of this Amended Complaint as if set forth fully herein.

160. Plaintiff brings this claim for relief against [24]7.ai on behalf of the Class.

161. **Violation of § 2701:** The Federal Stored Communications Act provides a private right of action against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." See 18 U.S.C. § 2701(a); see also 18 U.S.C. § 2707(a) (cause of action).

162. [24]7.ai was not necessary to Plaintiff and Members of the Class's purchase of tickets. Defendant [24]7.ai knew or should have known that its data security protocols were inadequate. It certainly knew this after the Data Breach occurred. Plaintiff and members of the Class certainly would not authorize [24]7.ai to access their information if known that [24]7.ai's security measures were inadequate, and most certainly would not authorize such access after the Data

Breach occurred.

163. During the wrongdoing herein alleged, [24]7.ai intentionally and without Plaintiff's and Class members' informed consent, accessed, found, copied and transmitted Plaintiff's and Class members' "electronic communications," even after the Data Breach occurred in violation of 18 U.S.C. §§ 2701(a), 2711(1).

164. **Violation of § 2702**: [24]7.ai violated the SCA by knowingly divulging the contents, including content and information, of Plaintiff's and Class members' electronic communications while they were in electronic storage to unauthorized parties, pursuant to 18 U.S.C. § 2702(a)(1).

165. [24]7.ai violated the SCA by knowingly divulging the contents, including content and information, of Plaintiff's and Class members' electronic communications that were carried or maintained on Delta's remote computing service to unauthorized parties, pursuant to 18 U.S.C. § 2702(a)(2).

166. As a result of Defendant [24]7.ai's violations of the SCA, Plaintiff and Class have suffered injury, including but not limited to the invasion of Plaintiff's and Class's privacy and property rights, and have been placed at an imminent, immediate, and continuing risk of identity theft-related harm.

167. Plaintiff and Class members have been aggrieved by the intentional and unlawful acts of Defendant [24]7.ai. As a direct result of that wrongdoing, Defendants caused damage to Plaintiff and Class members.

168. Because of Defendant [24]7.ai's violations of the Stored Communications Act and pursuant to 18 U.S.C. § 2707(b)-(c), Plaintiff seeks statutory damages, costs and reasonable attorneys' fees on behalf of herself and Class members.

169. Plaintiff also seeks equitable relief ordering Defendants to delete the Customer Data.

COUNT VI

Violation of the Computer Fraud and Abuse Act,

18 U.S.C. §§ 1030 *et seq.* Against [24]7.ai and Delta

170. Plaintiff, individually and on behalf of all other Class members, alleges and incorporates herein by reference, each and every allegation contained in paragraphs 1 through 169, inclusive of this Amended Complaint as if set forth fully herein.

171. This claim is brought under the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030, *et seq*. (the "CFAA"). By virtue of Defendants' conduct set forth above, Defendants violated Section 1030(a)(2) of the CFAA, which specifically apply to anyone who:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
>
> …
>
> (C) information from any protected computer;

172. Paragraph (e) of this section provides Section (e) of the CFAA provides that:

> (2) the term "protected computer" means a computer--
>
> **…**
>
> (B) which is used in or affecting interstate or foreign commerce or communication, …

173. Defendants are liable under the CFAA, because their actions either: (1) intentionally caused damage, (section 1030(a)(5)(A)); (2) recklessly caused damage (section 1030(a)(5)(B)); or (3) simply caused damage (section 1030(a)(5)(C)). Under the Act, "damage" is defined to include "any impairment to the integrity or availability of data, a program, a system, or information," that causes "loss to 1 or more persons during any 1-year period . . . aggregating at least

$5,000 in value . . .” 18 U.S.C. §§ 1030(a)(5)(B)(i), (c)(4)(a)(i)(I), and 1030(e)(8).

174. As described above, Defendants failed to disclose the Data Breach to Plaintiff and the Class for over six months. [24]7.ai in particular had knowledge of the Data Breach for six months and failed to disclose the breach to Plaintiff and the Class. Delta failed to identify the breach for the six months between when it occurred and when it was disclosed to Plaintiff and the Class. Delta had knowledge of the breach for at least two weeks prior to disclosure. This unreasonable delay in disclosure magnified the chance that Plaintiff and the Class would be damaged.

175. Plaintiff’s and Class members’ computers are “protected computers” within the meaning of 18 U.S.C. § 1030(e)(2)(B). By accessing the internet, these computers are used in interstate commerce and communication.

176. Defendants placed cookies on the computers of Plaintiff and the Class members.

177. Plaintiff and Class members suffered damages as defined in 18 U.S.C. § 1030(e). As a direct result of Defendants’ conduct, the integrity of the Customer Data and information of Plaintiff and members of the Class have been impaired. Such impairment has caused and will cause losses aggregating to at least $5,000 in value in any one-year period to Plaintiff and Class members.

178. Because of Defendants’ violation of the CFAA and pursuant to 18 U.S.C. § 1030(g), Plaintiff seeks recovery of compensatory damages and injunctive relief on behalf of herself and Class members. The impairment Plaintiffs and members of the Class are suffering are ongoing. Equitable relief should be entered ordering Defendants to delete the Customer Data and any cookies placed on the personal computers of Plaintiff and members of the Class.

VI. PRAYER FOR RELIEF

179. WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Amended Complaint, respectfully requests that the Court

enter judgment in her favor and against Defendants as follows:

A. For an Order certifying the Class and State Classes as defined here, and appointing Plaintiff and her Counsel to represent the Class and the State Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Customer Data, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Plaintiff and Class members the type of Customer Data compromised;

D. For equitable relief compelling Defendants to delete Customer Data of Plaintiff and Class members retained by Defendants and to delete cookies placed upon the computers of Plaintiff and the Class members;

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. For an award of actual damages and compensatory damages, in an amount to be determined;

G. For an award of costs of suit and attorney's fees, as allowable by law; and

H. Such other and further relief as this court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Based on the foregoing, Plaintiff, on behalf of herself, and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated this 29th day of April, 2019.

Respectfully submitted,

KOHN, SWIFT & GRAF, P.C.

/s/ Denis F. Sheils
DENIS F. SHEILS (pro hac vice)
dsheils@kohnswift.com
BARBARA L. GIBSON (pro hac vice)
bgibson@kohnswift.com
1600 Market Street, Suite 2500
Philadelphia, PA 19103
Telephone: (215) 238-1700
Facsimile: (215) 238-1968

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
DEMET BASAR (pro hac vice)
basar@whafh.com
KATE McGUIRE (pro hac vice)
mcguire@whafh.com
270 Madison Avenue
New York, NY 10016
Telephone: (212) 545-4600
Facsimile: (212) 686-0114

TOSTRUD LAW GROUP, P.C.
JON A. TOSTRUD
jtostrud@tostrudlaw.com
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Facsimile: (310) 278-2640

Attorneys for Plaintiff Teresa J. McGarry and the Proposed Class